STRATEGY RESEARCH PROJECT

INTEROPERABILITY: THE CORNERSTONE OF INFORMATION WARFARE

BY

MR. GREGORY G. BARAC
Defense Mapping Agency

USAWC CLASS OF 1996
U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

INTEROPERABILITY: THE CORNERSTONE OF INFORMATION WARFARE

by

Mr. Gregory G. Barac

Mr. Robert F. Minehart, Jr.
Project Adviser

U.S. Army War College
Carlisle Barracks, Pennsylvania 17013

ABSTRACT

AUTHOR: Mr. Gregory G. Barac

TITLE: Interoperability: The Cornerstone of Information Warfare

FORMAT: Strategy Research Project

DATE: 12 April 1996 **PAGES:** 24 **CLASSIFICATION:** Unclassified

Information warfare has won the joint acceptance within DoD and may become the biggest threat faced by our nation. The great achievement of interoperability between information-based systems (e.g., computers) also introduced inherent risks and vulnerabilities, which is the cornerstone of information warfare. Information warfare includes the ability to exploit and dominate information made assessable through computers and communications. Should there be concern about these vulnerabilities? Absolutely. Modern societies depend upon these information-based systems to live and work. This paper introduces the recentness of information warfare and highlights some current issues, like who is leading the effort. The success of the information society to make their systems interoperate with other systems greatly increased the potentiality of information warfare. A review of the evolution of system interoperability highlights this phenomenon. As a result of being directly influenced by the industrial-age society, leaders over the age of forty may be too challenged to adequately grasp the issues of information warfare and may lead ineffectively.

INTRODUCTION

The term *Information-based system*, used throughout this paper, represents a composition of hardware and software components (i.e., computers, communications, programs, and data) that collectively perform a functional requirement. This paper suggests the achievement of interoperability between different information-based systems as being the cornerstone of information warfare. Issues regarding the definition of information warfare are presented and serve to introduce the currency of the topic. The modern information society is presented as being the impetus for the need for interoperability, the basis for information warfare. The vulnerabilities of information-based systems are described as inherent risks caused by interoperability. A discussion attributes system interoperability and information warfare on allowing the hierarchical military decision making structures to flatten horizontally. Lastly, this paper deals wholly with intuitive and basic ideas and capabilities obtained from open literature.

Is information warfare a viable threat to U.S. national security? Absolutely. Information warfare is a threat to the U.S. as well as to any other modern society. Over the past two years, there have been numerous penetrations by unknown intruders into major U.S. telecommunications carriers, Internet providers, international telephone and a variety of end-user systems.[1] A primary objective of information warfare is to exploit the trust and dependency on information-based systems using the ways and means of electronic warfare; command and control warfare; cover and deception; and psychological operations. A recent DoD report, recognizing the threat extended into the civil sector, recommended that a national policy be developed to deal with information warfare strategic issues on a broader approach (e.g., beyond the military).[2]

BACKGROUND

The concepts of information warfare are imperceptible to many since the functional components and battlefields are typically intangible and exist invisibly in virtual places

having names like *infosphere* and *cyperspace*. This may help to explain why there is still much skepticism about the concept and why some consider the topic to be hoopla and an extravagant publicity stunt intended to mislead and confuse. The term information warfare has been called a catchphrase, a fad, and a fascination to the exclusion of almost everything else like *maneuver warfare* and *mission-oriented tactics*[3]

Nevertheless, information warfare has won the joint acceptance among defense department echelons and has quickly become institutionalized through out the Services and certain Department of Defense (DoD) agencies. The Air Force was the first to create an Information Warfare Center through combining the secure communication portion of their Cryptologic Support Center with their Electronic Warfare Center.[4] Similarly, the DoD Joint Chiefs, Army, Navy, and defense intelligence agencies have created offices and obligated resources to work the issue, a remarkable event when considering the dramatic force reductions and budget cuts within DoD.[5] Information warfare courses have even been added to the curriculums at the senior level war colleges of the Army, Air Force and Navy. The military revealed their interest in information warfare back in 1981, the year after Alvin Toffler's book, *The Third Wave*, was published.[6] Toffler was subsequently asked to assist DoD in "reconceptualizing war in Third Wave terms" during the development of a new doctrine (AirLand Battle Doctrine) which was used during Desert Storm.[7] Toffler's book also introduced the now commonly used terms "infosphere" and "third wave."[8] More recently, his book *War and Anti-War* (1993), as well as Winn Schwartau's book, *Information Warfare: Chaos on the Electronic Highway*, are also attributed to inspiring more interest in the subject.

Articles on information warfare began appearing in military journals promptly after the Chairman of the Joint Chief of Staffs (CJCS), General Colin Powell, attributed the successes of Desert Storm to "information age warriors."[9] The CJCS then issued Memorandum of Policy Number 30 (MOP 30) setting forth definitions and relationships to guide the joint community in its thinking about information warfare, and command and

control warfare. A DoD Directive (TS3600.1) has been drafted that promulgates a policy for each Service to implement information warfare.[10]

While there may be remarkable jointness in discussing the significance and potential of information warfare, there appears to be less conformity in understanding and defining it. The growing number of articles published during recent years demonstrates the enthusiasm by the military strategists and analysts to define information warfare. Proposals continue to evolve and mold the definition into being *the* warfare of the twenty-first century.[11] Researching the subject reveals several previously established warfare doctrines such as: electronic warfare, command and control warfare, cover and deception, and psychological operations. This adds to the confusion, and supports the notion that the term is merely a catch-all phrase. The realm of information warfare includes political, economic, social, and industry functional activities and their interdependencies.[12] Realizing this explains why there is such a variety of interpretations of the subject.

There are several good reasons for the focus on understanding the ambiguity of the term. First, there is no single, national level authority designated as being responsible for defining it. However, without having a clearer understanding of the subject, it is unrealistic to expect an appropriate expert to be designated to work the issue. The Commission on Roles and Missions of the Armed Forces reported the lack of a comprehensive, integrated approach for using information warfare to promote and protect U.S. national interest.[13] However, it offered no recommendations. Therefore, the quandary continues each time a different perspective is introduced and the definitions will continue to evolve chaotically until a principal source is identified who can systematically lead the development of the concept.

Second, most aspects of information warfare were considered highly sensitive to military vulnerabilities and capabilities, and remained classified within the Department of Defense, the leading authority on the subject, to protect national security. This prohibited open discussions on the subject. Lastly, each author derives his viewpoints from his

unique experiences and motivations when writing about this phenomenon, resulting in different interpretations.

It is unrealistic to expect a precise definition for a term having such a broad range. For example, you can imagine the difficulty a geologist, mathematician, chemist, biologist, and physicist would have agreeing on a single definition for the term "science" since each would define it respective to his discipline. The same difficulty is occurring in defining information warfare since it also encompasses multiple disciplines (e.g., command and control warfare, electronic warfare, psychological warfare, information processing), as well as different strategic, operational and tactical objectives.

Minimal research of the proliferation of articles concerning information warfare quickly reveals a common thread: the exploitation and domination of information, assessable through the technologies of computers and communications. This exploitation and domination of information include both defensive and offensive strategies. Through the sharing of information worldwide in near real-time, by way of the global information infrastructure (GII), information dominance has the potential of becoming a deterrence strategy of the future.[14] "The struggle to dominate the information sphere, the domain of command, control, communications, and intelligence (C^3I) will be the center of gravity of future conflicts between modern forces."[15]

Desert Storm was the first information war.[16] The use of information operations on the battlefield against Iraq represented a revolutionary change in military affairs.[17] The targeting of the Iraqi command and control as an order of first priority prohibited them from telling their forces when or where the coalition attack was coming.[18] At the strategic level, the use of information warfare deceived an entire Iraqi corps into thinking an amphibious operation was coming from the East. The knocking out of the Iraqi intelligence apparatus by the air campaigns maintained this deception and allowed a cover for two American Corps' and two allied divisions to move West for the ground attack. A Division conducted

raids against Iraqi forces in Wadi Al Batin to hold them while the main attack occurred farther West.

Preemptive political efforts by the coalition forces denied space-derived information to Saddam Hussein and ensured the dominance of space-dependent military capabilities, helping the coalition achieve decisive victory.[19] The French agreed to sell their Spot images of the Gulf only to those countries belonging to the coalition. Its images could have revealed critical intelligence about allied troop positions and movements.[20] However, EOSAT, operator of the Landsat satellites, insisted on maintaining its sales to non-coalition countries because of legal obligations.[21]

"The Iraqi leadership, conversely, approached war in so conventional and outmoded a fashion that it did not even exploit the space-base information potentially available to it."[22] This lopsided advantage in space has persuaded U.S. military analysts that such dominance in space should not be taken for granted. The weak link in the space control campaign was wrought by the West's appetite for war news.[23] The media's quest for information in the Gulf region tested the limits of the strict U.S. guidelines on the war coverage. CNN became the best source of intelligence for Iraqi leaders throughout the war. It provided up-to-date weather reports for the theater of operations; access to expert long-range and short-range military analysis; and viewer reactions from deep within America's heartland. "CNN business represented a real and potentially serious lapse in the space control mission."[24]

THE INFORMATION SOCIETY AND INTEROPERABILITY

We are living in an era of unprecedented innovations. It has been fifty years since the production of the first electrical digital computer, which was developed to support the military during World War II.[25] Since then, the remainder of this century has experienced the development of new technologies at a rate that no other civilization has in history. There should be no doubt that information systems technology has dramatically changed

everyday life in modern civilizations. There should also be agreement on the increased reliance and dependency on information-based systems. The daily transactions that modern societies depend upon to live and work as well as the supporting information infrastructures (e.g., utilities, telecommunication networks, transportation systems, banks, stock markets, media) have been entrusted to information-based systems.

This year (1996) marks the 50th anniversary of the U.S. military using computers, and the systems and capabilities have continued to evolve exponentially. It has been forty years since the first time in U.S. history that technical, managerial and clerical positions (e.g., white-collar) outnumbered industrial positions (e.g., blue-collar).[26] The U.S. is entering its *third* generation as an "information society" and therefore should be becoming more familiar with in understanding the phenomenon.[27] Workers that spend their days creating, using and distributing information are called "knowledge workers."[28]

The first generation, those born in the years 1956 through 1975, are currently 21 to 40 years old and make up over half of the workforce. The second generation, those born in the years 1976 through 1995, are the 1 to 20 year olds comprising the entire education system. The third generation, just beginning, is those who are born in the years 1996 to 2015. Perhaps then, the recent escalation of trying to understand the phenomenon of information warfare is attributed to the senior leadership population being above the age of forty. That is, this group, having been directly influenced by industrial age experiences, may be too challenged to effectively lead an information society. Yet, those in their early forties and anyone who help initiate the information age, may be better prepared to lead an information society.

The wide range of technologies based on applications of the integrated circuit is referred to as information systems technology.[29] The committed research, development and use of increasingly more powerful processors over the last two decades led to the integration of three previously different technologies: data processing, communications and office equipment. Once manufacturers began incorporating new features permitted by

integrated circuits, the distinctions between these technologies began to blur. A frenzied competition ensued as each manufacturer tried to capture the exploding market for their information systems. Unfortunately, the competition encouraged the development of proprietary hardware and software designs.

While consumers were initially satisfied the equipment met their needs, the proprietary designs soon became the cause of several problems. One problem was that the consumers found themselves trapped in expensive, non-competitive maintenance contracts with the equipment manufacturers. The maintenance of information systems equipment quickly became major annual budget items. Another problem was that the systems were not compatible with other systems. In other words, systems manufactured by different vendors could not communicate with each other and exchange information electronically. This problem was an intolerable situation with the information society and quickly established the need for standards (i.e., protocols) for software and hardware designs.

Realizing the magnitude of this problem, the Assistant Secretary Defense (ASD) for Command, Control, Communications and Intelligence (C^3I), Emmett Paige, stated the following a speech to the Communications and Electronics Association on Aug. 22, 1995:[30]

> We have been burned in the past by the acquisition of vendor proprietary systems that represented the best value for the money at the time, but whose upgrades proved too costly as time and technology advanced. We have learned our lesson -- standardize the interfaces, using commercial standards whenever possible to create a systems environment in which individual creativity can flourish, so the component software and hardware systems can rapidly evolve and be integrated into a stable matrix of interoperable systems at minimum cost and downtime...Competing vendors often inject proprietary designs in their products without regard to interoperability standards, which then render them incompatible with other network components. Competition among firms developing similar technologies is fierce.

The evolution of the computer demonstrates that a great amount of effort was spent to keep systems incompatible (e.g., unable to exchange data electronically). As senseless as this may seem, it was an intentional motive stemming from the competitiveness between

the computer manufacturers in their attempts to ensure their intellectual property rights and secure a share of the market.

For example, the use of the $Base_2$ numbering system (i.e., using only the digits 1 and 0) to represent a binary digit (bit) was the universal principle followed by all computer manufacturers worldwide. What was not universal, however, was the combination of bits used to represent the data. At the outset, computer manufacturers developed their own proprietary code representations (derived from the original International Telegraph Alphabet developed by the French telegrapher, Baudot).[31] This caused inherent limitations of exchanging data between systems since computer software (and digitized data) was wholly dependent on a specific manufacturer's processors and unusable on another manufacturer's processors.

The incompatibility problems led to the development of the 1963 standard called the American Standard Code for Information Interchange (ASCII).[32] By end of the 1970s, the entire computer industry had converted their systems to ASCII (except IBM who continues to maintain their proprietary code Extended Binary Code Decimal Interchange Code (EBCDIC), on their mainframe computers). To compensate for these differences, electronic translators were designed into most input/output processors to convert ASCII to EBCDIC and vice versa. The use of ASCII to standardize the encoding of digitized data was a giant step toward allowing data to be exchanged between computers.

However, there were still obstacles that prohibited the communication between unlike computers. The uniqueness between the multiple layers of system interfaces (e.g., operating systems, input/output processors, application programs, electronic signals) had to be addressed. This required extensive hardware and software engineering efforts that initiated the requirement for national and international communications standards (i.e., protocols). Establishing communications protocols was a colossal task involving more than a decade of negotiations between the computing and communication industries, international electrical engineers' associations and governments throughout the 1980s.

The main issues were primarily costs, data integrity, network reliability, and system performance.

The military was particularly concerned with network reliability and survivability from a physical attack. This requirement led to the development of packet-switching which permitted the linking of computers in distant geographic locations. Packet-switching offered a way of maintaining the integrity of the military command-and-control network in case of a nuclear attack. In 1969, the Advanced Research Projects Agency (ARPA) funded a large-scale test of this concept to access other computer facilities over long distances with remote terminals. By 1971, users were heavily using the dedicated, high-speed, computer network as an electronic post office. Because of its distributed structure, expansion of the network was easy and it grew rapidly. In 1983, the ARPA network (ARPANET) split away from the military's similarly designed Defense Data Network (DDN), and grew into what is known today as the Internet.

The communication protocol controversy did not result in a solution of one protocol. Instead, the International Standards Organization (ISO) approved a variety of protocols (e.g., 802.5 token ring, 802.3 ethernet, FDDI, etc.). This compromise permitted the manufacturers and their customers to continuing using their existing equipment (e.g., miles of cables, and thousands of computer terminals and mainframe computers). The establishment of communication protocols permitted all manufacturers to design compatible hardware and software interfaces to the other protocols since they now knew the design specifications and thus opening a new market. Specialized communication processors, called gateways, could then be developed to translate between different network protocols (similar to EBCDIC - ASCII translators).

The requirements by the U.S. military acquisitions were typically non-standard which continued to cause information systems to be incompatible between the services. The Vice Chairman of the Joint Chiefs of Staff, Admiral Owens, stressed the necessity for weapons and systems, in or entering U.S. military inventories, to be reviewed for their

requirement to interoperate with other systems.[33] In addition, the ASD C^3I, Emmett Paige, stated (in the same speech cited previously):[34]

> It is a known fact that DoD still has a sizable inventory of C4I systems which are legacy in nature and stovepiped in function, as they do not interoperate with other systems. In October 1993, Deputy Secretary of Defense Perry imposed a three-year deadline to minimize the number of duplicative DoD information support systems and make the remaining migration set interoperable.

INHERENT VULNERABILITIES

> Information has become perhaps the world's fastest growing and most important businesses. The spy is a living symbol of the revolution now sweeping the infosphere.
>
> - Alvin Toffler (1980)[35]

The open systems architecture and commercial off-the-shelf (COTS) system components described earlier, greatly increase the vulnerabilities of information-based systems. The risk of using open architecture interface standards and protocols is inherent within the design of being "open". The very objective of the architecture is to permit access to the design specifications (e.g., electrical and logical) of the specified protocol. Therefore, anyone with the appropriate technical experience can easily construct a system that will interface with other systems. "Because the private sector is leading the development and marketing of information age technologies, the technological leveling has accelerated as emergent technologies are made available to anyone with sufficient resources."[36]

Information-based systems are vulnerable to a multitude of forces. Vulnerabilities include any method such as the use of computer viruses and Trojan horses that disrupt information-based systems. Some disruptions result from unintentional acts such as human operator errors, software bugs, hardware component failures, or natural events causing loss of power (e.g., weather, earthquake, flood). Other causes, however, may be malicious attacks.

Information-based systems run on pre-established logic, or instructions referred to as a program or software. Software, invisible within information-based systems, is the link between all information processes, as it powers the flow of all digital data controlling images, messages, or guiding precision guided weapons. Software, comprehensible only to programmers or software engineers, is a sequence of instructions designed to execute conditionally. It has no loyalties nor can it be swayed by changing ideals, and can work consistently and relentlessly as long as required, without supervision. It is corruptible and susceptible to threats such as design errors (e.g., bugs) of poor logic, interface incompatibilities, or computer viruses and Trojan horses introduced externally.

The vulnerabilities are so great that DoD employs a strict discipline known as information systems security (INFOSEC) which is dedicated to ensuring the trustworthiness of information systems. The DoD INFOSEC policy states that any automated information system that processes classified, sensitive unclassified, or unclassified information must undergo a technical analysis and management approval before it is allowed to operate.[37] The technical analysis, or certification, establishes the extent to which a system meets a set of specified security requirements for its purpose and operational environment. The management approval, or accreditation, is the formal acceptance of responsibility for operating at a given level of risk. These concepts are quite general and are applied with different levels of formality within different organizational structures.[38]

The dependency on economic and civil uses of information-based systems makes it very likely these systems will be targeted in an information war. The resolutions of the interoperability issues have opened the flood gates of information transferability. "Attacks on the United States and its information infrastructure, be they part of a larger conflict, state-sponsored terrorism or merely electronic mugging, can now be mounted without regard to the physical boundaries on which we have relied for over 200 years."[39] "We have been slow as a nation to realize that the temporal and geographical sanctuary that the

United States has always enjoyed has been lost."[40] "The sense of sanctuary lost, of personal privacy denied, and of a collective public safety at risk, has been reinforced by such diverse events as the Oklahoma City and World Trade Center bombings, the collapse of a British bank due to actions of a single trader resident in Singapore, amid the growing awareness of the 'hacker/cracker' community's ability to penetrate and manipulate data."[41]

There is no national level, overarching authority accountable for pursuing the development and implementation of an information assurance policy. A recent DoD report recommended a national policy be developed dealing with information warfare strategic issues on a broader approach, extending beyond military into the civil sector.[42]

The risk of provocation and information attacks is imminent. "Both the public and private sectors have been slow to acknowledge and deal with information age deliberate attacks, unintended consequences, accidents or natural disasters."[43] Hackers have gained access to sensitive government and commercial computer systems.

CONCLUSION

> To discover how much of our resources must be mobilized for war...we must gauge the strength and situation of the opposing state... character... government... people... abilities... political sympathies of other states and the effect the war may have on them...to assess these things in all their ramifications and diversity is plainly a colossal task... rapid and correct appraisal of them clearly calls for the intuition of a genius... to master all this complex mass by sheer methodical examination is obviously impossible. Bonaparte was quite right when he said that Newton himself would quail before the algebraic problems it could pose.
>
> - Carl von Clausewitz[44]

While this was unequivocally valid nearly two centuries ago, a rapid and correct appraisal of such a colossal task is no longer an impossibility today. The "intuition of a genius" is easily duplicated by information-based systems that can methodically examine a complex mass and perform an array of algebraic problems in fractions of a second.

The Air Force Chief of Staff, General Ronald R. Fogleman, indicated the next fifteen years will see a tremendous potential for breakthrough with the ability to exploit and

exchange information and to detect, fix and target objectives on a battlefield.[45] It will be information, and the capability to move it around, that will change the internal characteristics of ships, aircraft, battle tanks and armored personnel carriers.[46] During the last half of this century, modern societies have experienced technological changes in revolutionary proportions. Information-based systems have evolved extraordinarily since the production of the first computer that improved the speed and accuracy of targeting calculations during World War II. Who would have predicted that the computer itself would become a strategic weapon and target for future conflicts? Visionaries and alarmist have inspired and even assisted in the development of new battlefield operations and tactics, using enhanced computer and telecommunication technologies, and command and control warfare strategies.

A principle to be followed by the employment of U.S. forces in war is to help dominate combat operations by winning the information war.[47] This suggests the strategic use of information warfare is that of a force multiplier. Which is supported by the CJCS statement "a downsized force and a shrinking defense budget result in an increase reliance on technology, which must provide the force multiplier required to ensure a viable military deterrent."[48] It must be noted, however, that adopting information technologies as force multipliers without changing the way business is done may be the greatest single threat faced by the services.[49]

Recent organization and management theory innovations represent changing paradigms. Informational bottlenecking has always been a vulnerability in centralized, hierarchical structures for command and control. "The information revolution reflects the advance of the computerized information and communications technologies and innovations in organization and management theory."[50] Innovations in organizational designs are changing traditional stovepipe hierarchies to flatter network-oriented models allowing greater flexibility, lateral connectivity, and teamwork across institutional boundaries. "In Clausewitz's sense, it is characterized by the effort to turn knowledge into capability."[51]

The emphasis on command and control is giving way to coordination and team work, the building blocks of networked designs.

Operational and tactical command may become exceptionally demanding. Leaders at all levels will operate with greater latitude. Instead of divisions, brigades, and battalions, cyberwar may require the creation of combined-arms task forces from each of the services.[52] Just as computers have flattened the organizational charts of corporations, the military may have to restructure its ranks. Fewer layers of staff officers are needed to process orders between a general and his shooters on the ground.[53]

Information warfare is not isolated to computers, communications and system interoperabilities, as was the primary focus in this paper. It comprises a diverse field of other arts and sciences such as electronics, psychological, military and economics. The continued simplicity of availability and interoperability of information-base systems introduce inherent opportunities as well as vulnerabilities and risks. Modern societies reliance on information-based systems built with commercial off-the-shelf hardware and software platforms using open architecture interface standards introduces risks that are nearly impossible to guard against, by the very nature of the requirement of systems to interoperate with other systems. It is extremely difficult to conduct an information war without expert knowledge of the opponent's information architecture. Knowledge is required ranging from how the media influence decisions, to the bureaucratic structure of command, to a nation's communications infrastructure, and even the details of their information systems' software.[54]

System interoperability and information warfare facilitate flattening the organization and will revolutionize the ancient hierarchical chain-of-command institution. Having a total picture of the battlefield and the ability to run tactical simulations while communicating with joint and combined forces, allows the combatant to make informed decisions without going through multitudes of staff layers.

Finally, the interagency process supporting the National Command Authority is not organized to deal with technology based threats.[55] A national civil defense structure, composed of citizens trained and experienced in technical skills (e.g., computers, communications, and electrical engineering) is required. This structure would be capable and responsible for ensuring our national security by responding to the technological threats imposed by an information war.

END NOTES

[1] George J. Stein, "Information Warfare," Airpower Journal, IX,no.1 (Spring 1995): 2-7.

[2] A Research Report for the: Chief, Information Warfare Division (J6K) Command, Control, Communications and Computer Systems Directorate Joint Staff, 4 July 1995, 1-1.

[1] R. L. DiNardo and Daniel J. Hughes, "Some Cautionary Thoughts on Information Warfare," Airpower Journal (Winter 1995): 69.

[4] "EW Expands Into Information Warfare," Aviation Week & Space Technology, 10 October 1994, p. 47.

[5] U.S. Department of Defense. "Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance," A Research Report for the: Chief, Information Warfare Division (J6K) Command, Control, Communications and Computer Systems Directorate Joint Staff. Prepared by Science Applications International Corporation (SAIC), 4 July 1995, A-14, A-16.

[6] Alvin Toffler and Heide Toffler, War and Anti-War (New York: Warner Books, Inc., 1993): 7-11. Soon half after The Third Wave was published, Alvin Toffler was asked to meet with Generals Don Morelli and Donn Starry to help "reconceptualizing war in Third Wave terms" in their efforts of formulating the military AirLand Battle Doctrine.

[7] Ibid.

[8] Alvin Toffler, The Third Wave, (New York: Bantam Books, Inc., 1980): 125-363.

[9] Colin L. Powell, "Information-Age Warriors," BYTE, July 1992, p. 370.

[10] Wayne J. Rowe, "Information Warfare: A Primer for Navy Personnel," Strategic Research Department Research Report, June 1995, 28.

[11] Martin C. Libicki, "What is Information Warfare," Strategic Forum 28 (May 1995): 1. Libicki proposed the following: 1) Command-and-Control Warfare [C2W]; 2) Intelligence-Base Warfare [IBW]; 3) Electronic Warfare [EW]; 4) Psychological Operations [PSYOPS]; 5) Hackerwar-software-based attacks on information systems; 6) Information Economic Warfare [IEW] - war via the control of information trade; 7) Cyberwar (combat in the virtual realm).

[12] A Research Report for the: Chief, Information Warfare Division (J6K) Command, Control, Communications and Computer Systems Directorate Joint Staff, 4 July 1995, 2-3.

[13] U.S. Department of Defense, "Directions for Defense,." Report of the Commission on Roles and Missions of the Armed Forces, May 1995, 2-15.

[14] George M. Moore, Vic Budura and Joan Johnson-Freese, "Joint Space Doctrine: Catapulting into the Future", Joint Force Quarterly (Summer 1994): 73.

[15] Mark Lewonowski, "Information War," In Essays On Strategy IX, ed. Thomas C. Gill, (Washington: National Defense University, 1993), 55.

[16] Edward Mann, "Desert Storm: The First Information War?" Airpower Journal, (Winter 1994): 1.

[17] Frederik M. Franks Jr., "Winning the Information War: Evolution and Revolution," Vital Speeches of the Day 60 (May 1994):455.

[18] Ibid.,456.

[19] Steven Lambakis, "The World's First Space War," Orbis 39 (Summer 1995): 417.

[20] Ibid.,421.

[21] Ibid.

[22] Ibid.,418.

[23] Ibid.,422.

[24] Ibid.

[25] Grolier Multimedia Encyclopedia, V7.0.2 (Grolier Electronic Publishing Inc., 1995), s.v. "Computers" by Robert Swanson. World War II produced a desperate need for computing capability. New weapons systems required accurate trajectory tables and other essential data. To meet this need, a team led by Eckert and Mauchly at the Moore School of Electrical Engineering of the University of Pennsylvania built a high-speed electronic computer named the Electronic Numerical Integrator and Computer (ENIAC). The ENIAC could compute about 300 products per second by finding the value from a multiplication table stored in its memory. It used 18,000 vacuum tubes, occupied 1,800 square feet of floor space, and required 180,000 watts of electricity. The ENIAC is generally acknowledged to be the first successful high-speed electronic digital computer and was productively used from 1946 to 1955.

[29] John Naisbitt, Megatrends, (New York: Warner Books, 1982); quoted in George W. Reynolds, Information Systems For Managers 2d ed., (St. Paul: West Publishing Co., 1992), 5.

[27] Ibid.

[28] Ibid.,6.

[29] George W. Reynolds, Information Systems For Managers 2d ed., (St. Paul: West Publishing Co., 1992), 4.

[30] Paige, Emmett Jr. "Retaining the Edge on Current and Future Battlefields Defense." Defense Issues (August 1995): 4.
URL: http://www.dtic.dla.mil/defenselink/pubs/di_index.html.

[31] Ken Sherman, Data Communications- A Users Guide 3rd ed., (New Jersey: Princeton Hall., 1990), 571.

[32] In 1977 the American National Standards Institute (ANSI) adopted ASCII as standard "X3.4".

[33] William A. Owens. "The Emerging System of Systems," Military Review 9 (May-June 1995): 15-19.

[34] Paige, 4.

[35] Alvin Toffler, The Third Wave (New York: Bantam Books, Inc., 1980), 156.

[36] Oscar W. Round and Earle L. Rudolph, Jr., "Civil Defense in the Information Age," Strategic Forum 46 (September 1995): 2.

[37] National Computer Security Center, Introduction to Certification and Accreditation (Ft. George G. Meade: National Computer Security Center, 1994), 1.

[38] Ibid.

[39] Ibid.

[40] Ibid.

[41] Ibid.

[42] A Research Report for the: Chief, Information Warfare Division (J6K) Command, Control, Communications and Computer Systems Directorate Joint Staff, 4 July 1995, 1-1.

[43] Round, 2.

[44] Carl von Clausewitz, On War, Translated by Sir Michael Howard and Peter Paret, (Princeton: Princeton University Press, 1976): 585-586.

[45] Ronald R Fogleman, "What Information Warfare Means To You," Air Force Times, 17 July 1995, p. 31.

[46] Ibid.

[47] 1995 National Military Strategy, ii.

[48] Powell, 370.

[49] Stein, 32.

[50] John Arquilla and David Ronfeldt, "Cyberwar is Coming," Comparative Strategy 12 (1993): 143.

[51] Ibid.,147.

[52] Ibid.,156.

[53] Douglas Waller, "Onward Cyber Soldiers", Time, 21 August 1995, p. 44.

[54] Libicki, 4.

[55] Round, 3.

BIBLIOGRAPHY

Ackerman, Robert K. "Military Planners Gird For Information Revolution." Signal 49 (May 1995): 71-79.

Ailes, Robert H. "Exploiting the Commercial Information-Management Revolution." Sea Power (April 1992): 97-103.

Alexander, David. "Information Warfare and the Digitized Battlefield." Military Technology 19 (September 1995): 57-64.

Alford, Kenneth L. "DoD and the Global Information Infrastructure." CrossTalk (August 1995): 7-9.

Arquilla, John. "Strategic Implications of Information Age." Strategic Review 22 (Summer 1994): 24-30.

_____ and David Ronfeldt. "Cyberwar is Coming." Comparative Strategy 12 (1993): 141-165.

Berkowitz, Bruce D. "Warfare in the Information Age." Issues in Science and Technology (Fall 1995): 61.

Campen, Alan D. "Rush to Information-base Warfare Gambles with National Security." Signal 49 (July 1995): 67-69.

Clapper, James R. and Eben H. Trevino. "Critical Security Dominates Information Warfare Moves." Signal 49 (March 1995): 71-72.

Clausewitz, Carl von. On War. Translated by Sir Michael Howard and Peter Paret. Princeton: Princeton University Press, 1976.

Clodfelter, Mark and John M. Fawcett. "RMA and Air Force Roles, Missions, and Doctrine." Parameters 25 (Summer 1995): 22-29.

Deutch, John. "Toward A Better Intelligence Community Relationshiop." Defense Issues 10, no.73 (July 1995): 1-4.

"Digitized Zephyr Lifting Fog From No Man's Land." National Defense, 80 September 1995, 32-33.

DiNardo, R. L. and Daniel J. Hughes. "Some Cautionary Thoughts on Information Warfare." Airpower Journal (Winter 1995): 69-79.

"EW Expands Into Information Warfare." Aviation Week & Space Technology, 10 October 1994, 47-48.

Felker, Ed. "Information Warfare: A View of the Future." A Common Perspective - Joint Warfighting Center's Newsletter 3 (September 1995): 17-18.

Fogleman, Ronald R. "What Information Warfare Means To You." Air Force Times, 17 July 1995, 31.

_____. "Information Operations: The Fifth Dimension of Warfare." Defense Issues, no. 47 (1995): 1-3.

Franks, Frederik M. Jr. "Winning the Information War: Evolution and Revolution." Vital Speeches of the Day 60 (May 1994): 453-458.

Funk, Paul E. "The Army's 'Digital Revolution'." Army (February 1994): 33.

Gambel, Daniel. "MLS (Multi-Level Security): Data Security for the DoD and the Rest of Us." Defense Electronics 27 (June 1995): 10.

"Going Beyond Real-Time The Next Step in Simulation." Aviation Week & Space Technology, 12 September 1994, 71.

Goodman, Glenn W. "Power of Information: Air Force Clarifies its Misunderstood Virtual Presence Concept." Armed Forces Journal International 132 (July 1995): 24.

Grier, Peter. "Information Warfare." Air Force Magazine 78 (March 1995): 34-37.

Hunter, Roger C. "Disabling Systems and the Air Force." Airpower Journal VIII, no.3 (Fall 1994): 43-47.

Jensen, Owen E. "Information War: Principles of Third-Wave War." Airpower Journal 8 (Winter 1994): 35-43.

Johnson, Craig L. "Information Warfare: Not a Paper War." Journal Of Electronic Defense 17 (August 1994): 55-56.

Jones, Jeffrey B. "Theater Information Strategies." Military Review 74 (November 1994): 48-50.

Kabay, M. E. "Prepare Yourself For Information Warfare." Computerworld - Leadership Series, 20 March 1995, 2-7.

Kraus, George F. "Information Warfare in 2015." U.S. Naval Institute Proceedings, 121 (August 1995): 42-45.

Lambakis, Steven. "The World's Fist Space War." Orbis 39 (Summer 1995): 417-433.

"Leveraging the Infosphere: Surveillance and Reconnaissance in 2020." Airpower Journal 9 (Summer 1995): 8-25.

Lewonowski, Mark C. "Information War." In Essays On Strategy IX, ed. Thomas C. Gill, 55-80. Washington: National Defense University, 1993.

Libicki, Martin C. "What is Information Warfare?" Strategic Forum 28 (May 1995): 1-4.

Mahanna, Cory W. And James Gagliarducci. "Army Aviation Bridges Communications on the Battlefield." Military Review 75 (May-June 1995): 42-45.

Mann, Edward. "Desert Storm: The First Information War?" Airpower Journal 8 (Winter 1994): 4-13.

Marshall, Joe, John Thau and Richard Waddell. "Computer Systems." Aerospace America (December 1994): 38-39.

Matthys, Erick T. "Harnessing Technology for the Future." Military Review 75 (May-June 1995): 71-76.

Moore, George M., Vic Budura and Joan Johnson-Freese, "Joint Space Doctrine: Catapulting into the Future." Joint Force Quarterly. (Summer 1994): 71-76.

Morris, Chris, Janet Morris and Thomas Baines. "Weapons of Mass Protection: Nonlethality, Information Warfare, and Airpower in the Age of Chaos." Airpower Journal 9 (Spring 1995): 15-29.

Munro, Neil. "Infowar Disputes Stall Defense Policy." Washington Technology. 25 May 1995, 40.

Naisbitt, John. Megatrends. New York: Warner Books, 1982. Quoted in George W. Reynolds. Information Systems For Managers 2d ed.,5-6, St. Paul: West Publishing Co., 1992.

Nelson, David B. Information-based Warfare: an annotated bibliography. Washington: National Defense University, 1994.

Owens, William A. "Four Revolutions In Military Thinking." The Officer (August 1995): 29-44.

_____. "The Emerging System of Systems." Military Review 9 (May-June 1995): 15-19.

Paige, Emmett Jr. "Retaining the Edge on Current and Future Battlefields Defense." Defense Issues (August 1995). Internet World Wide Web URL: http://www.dtic.dla.mil/defenselink/pubs/di_index.html.

Perry, William J. "Linking Technology and National Security." Defense Issues 10, no.71 (June 1995): 1-2.

_____. "Annual Report to the President and the Congress." (Washington: Government Printing Office, 1995), 263-64.

Powell, Colin L. "Information-Age Warriors." BYTE, (July 1992): 370.

Reynolds, George W. Information Systems For Managers. 2d ed. St. Paul: West Publishing Co., 1992.

Robinson, Clarence A. "Electronic Combat Techniques Provide Information War Edge." Signal (July 1995): 33-37.

Ross, Philip E. and Nikhil Hutheesing. "Along Came The Spiders." Forbes, 23 (October 1995): 210-216.

Ross, Jimmy D. "Winning the Information War." Army 44 (February 1994): 27-32.

Round, Oscar W. and Earle L. Rudolph, Jr. "Civil Defense in the Information Age." Strategic Forum 46 (September 1995): 1-4.

Rowe, Wanyne J. "Information Warfare: A Primer for Navy Personnel." Strategic Research Department Research Report. U.S. Naval War College, June 1995.

Ryan, Donald E. "Implications of Information-Based Warfare." JFQ: Joint Force Quarterly 6 (Autumn/Winter 1994-95): 114-116.

Schwartau, Winn. Information Warfare: Chaos on the Electronic Superhighway. New York: Thunder's Mouth Press, 1994.

Scott, Alvin. "Intelligence, Beyond 2010." Military Intelligence, (April-June 1995): 41-43.

Scott, William B. "'Information Warfare' Demands New Approach." Aviation Week & Space Technology, 13 March 1995, 85-88.

Sherman, Ken. Data Communications- A Users Guide 3rd ed. New Jersey: Princeton Hall, 1990.

Smith, Edward A. "Putting it Through the Right Window." U.S. Naval Institute Proceedings, 121 (June 1995): 38-40.

Stein, George J. "Information Warfare." Airpower Journal 9 (Spring 1995): 30-39.

Stocker, Lee. "The Army Joins the Web." Crosstalk (July 1995): 30-31.

Struble, Dan. "What is Command and Control Warfare." Naval War College Review 48 (Summer 1995): 89-98.

Sullivan, Gordan R. and James M. Dubik "War In The Information Age", U.S. Army War College Strategic Studies Institute, 6 June 1994, 145-159.

Swanson, Robert. "Computers." Grolier Multimedia Encyclopedia, 7.0.2, 1995.

Swett, Charles. "Review Essay: War and Anti-War." Special Warfare 8 (January 1995): 26-29.

Szafranski, Richard. "A Theory of Information Warfare: Preparing for 2020." Airpower Journal 9 (Spring 1995): 56-65.

Toffler, Alvin. The Third Wave. New York: Bantam Books, Inc., 1980.

_____ and Heide Toffler. War and Anti-War. New York: Warner Books, Inc., 1993.

U.S. Congress, Office of Technology Assessment (OTA Report Summary). "Information Security and Privacy in Network Environments." September 1994.

U.S. General Accounting Office. Report to the Chairman, Government Information, Justice, and Agriculture Subcommitee, Committee on Government Operations, House of Representatives; Computer Security: DEA Is Not Adequately Protecting National Security Information Washington: U.S. General Accounting Office, 1992.

U.S. Department of Defense, Defense Science Board. Report of the Defense Science Board Summer Study Task Force on Information Architecture For the Battlefield.

(Washington: Office of the Undersecretary of Defense For Acquisition & Technology, October 1994), B-16

U.S. Department of Defense. "Directions for Defense." Report of the Commission on Roles and Missions of the Armed Forces. May 1995.

U.S. Department of Defense. "Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assuranc." A Research Report for the: Chief, Information Warfare Division (J6K) Command, Control, Communications and Computer Systems Directorate Joint Staff. Prepared by Science Applications International Corporation (SAIC), 4 July 1995.

U.S. National Security Agency. Introduction to Certification and Accreditation. Ft. George G. Meade: National Computer Security Center, 1994.

Waller, Douglas. "Onward Cyber Soldiers." Time, 21 August 1995, 44.

Walsh, Robert S. "Information Enhancement on Today's Battlefield." Marine Corps Gazette, October 1995, 27-29.

Wardynski, E. Casey. "Labor Economics of Information Warfare." Military Review, 75 (May-June 1995): 56-61.

Williamson, John. "Winning the Data War." Jane's Defense Weekly 23 (May 1995): 44-46.

Wilson, G.I. and Frank Bunkers. "Uncorking the Information Genie." Marine Corps Gazette, October 1995, 29-31.